ETSI TS 129 283 V13.1.0 (2016-08)

LTE;
Universal Mobile Telecommunications System (UMTS);
Diameter data management applications
(3GPP TS 29.283 version 13.1.0 Release 13)

Reference
RTS/TSGC-0429283vd10

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This 3GPP Technical Specification (TS) specifies:

1. The interactions between the MCPTT User Database and the MCPTT Server. This interface is referred to as the MCPTT-2 reference point.
2. The interactions between the MCPTT User Database and the Configuration Management Server. This interface is referred to as the CSC-13 reference point.

The functional architecture for support of mission critical communication services is specified in 3GPP TS 23.179 [2].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2".

[3] IETF RFC 3588: "Diameter Base Protocol".

[4] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[5] IETF RFC 4960: "Stream Control Transmission Protocol".

[6] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[7] IETF RFC 5234:"Augmented BNF for Syntax Specifications: ABNF".

[8] IETF draft-ietf-dime-drmp-03: "Diameter Routing Message Priority".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[9] 3GPP TS 29.329: "Sh interface based on the Diameter protocol; Protocol details".

[10] 3GPP TS 29.336: "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications".

[11] IETF RFC 7683: "Diameter Overload Indication Conveyance".

[12] 3GPP TS 23.003: "Numbering, addressing and identification".

[13] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] IETF RFC 3986:"Uniform Resource Identifier (URI): Generic Syntax".

[16] 3GPP TS 24.384: "Mission Critical Push To Talk (MCPTT) configuration management; Protocol specification".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply, if any.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], in 3GPP TS 23.179 [2] and the following apply, if any. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

4 Main Concept

4.1 Introduction

The MCPTT-2 reference point (between the MCPTT Server and the MCPTT User Database) and the CSC-13 reference (between the Configuration Management and the MCPTT User Database) are defined in the 3GPP TS 23.179 [2].

This document describes the Diameter-based MCPTT-2 and CSC-13 related procedures, message parameters and protocol specification.

This document specifies the Diameter Management Application used as protocol over the MCPTT-2 and CSC-13 reference points.

5 MCPTT General Architecture

5.1 Introduction

This section further specifies the architectural assumptions associated with the MCPTT-2 and CSC-13 reference points, building on 3GPP TS 23.179 [2].

5.2 Functional requirements of network entities

5.2.1 Functional Requirements of the MCPTT Server

The MCPTT Server may communicate with the MCPTT User Database over the MCPTT-2 interface.

For more details on the functionality of the MCPTT Server, refer to 3GPP TS 23.179 [2].

5.2.2 Functional Requirements of the Configuration Management Server

The Configuration Management Server may communicate with the MCPTT User Database over the CSC-13 interface.

For more details on the functionality of the Configuration Management Server, refer to 3GPP TS 23.179 [2].

5.2.3 Functional requirements of MCPTT User Database

The MCPTT User Database may communicate with the MCPTT Server over the MCPTT-2 interface.

The MCPTT User Database may communicate with the Configuration Management Server over the CSC-13 interface.

For more details on the functionality of the MCPTT User Database, refer to 3GPP TS 23.179 [2].

5.3 Functional classification of MCPTT-2 interface procedures

Operations on the MCPTT-2 interface are classified in functional groups:

1. Data handling procedures

    - The download of data from the MCPTT User Database to an MCPTT Server.
    - The subscription to notifications from the MCPTT User Database when particular information about a specific MCPTT User is updated.
    - The MCPTT User Database can notify an MCPTT Server of changes in data for which the MCPTT Server previously had subscribed.

5.4 Functional classification of CSC-13 interface procedures

Operations on the CSC-13 interface are classified in functional groups:

1. Data handling procedures

    - The download of data from the MCPTT User Database to a Configuration Management Server.
    - The update of data in the MCPTT User Database.
    - The subscription to notifications from the MCPTT User Database when particular information about a specific MCPTT User is updated.
    - The MCPTT User Database can notify a Configuration Management Server of changes in data for which the Configuration Management Server previously had subscribed.

6 Procedure Descriptions for MCPTT

6.1 Introduction

This clause describes the procedures invoked between:

- the MCPTT Server and the MCPTT User Database over the MCPTT-2 reference point;
- the Configuration Management Server and the MCPTT User Database over the CSC-13 reference point.

In the tables that describe the Information Elements transported by each command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional in the "Cat." column. For the correct handling of the Information Element according to the category type, see the description detailed in subclause 6 of the 3GPP TS 29.228 [14].

6.2 MCPTT User data handling procedures

6.2.1 Data Pull

6.2.1.1 General

This procedure is used between the MCPTT Server or the Configuration Management Server and the MCPTT User Database.

The procedure is invoked by the MCPTT Server or the Configuration Management Server and is used:

- To obtain information about a specific MCPTT User from the MCPTT User Database;

- To subscribe to notifications from the MCPTT User Database for when particular information about a specific MCPTT User is updated.

This procedure is mapped to the commands Data-Pull-Request/Answer in the Diameter application specified in subclause 7.2.3/7.2.4. The tables 6.2.1-1 and 6.2.1-2 detail the involved information elements.

Table 6.2.1-1: Data Pull Request

Information element name	Mapping to Diameter AVP	Cat.	Description
MCPTT ID	User-Identifier (See 7.3.8)	M	This information element contains the MCPTT ID of the user for whom the data is required. See 3GPP TS 23.179 [2]. See subclause 7.3.8 for the content of this AVP.
Requested Data	Data-Identification (See 7.3.3)	M	This information element indicates the requested information. The set of valid values are defined in subclause 7.3.3.
DPR Flags	DPR-Flags (See 7.3.13)	O	This information element contains one or several flags that define different command behaviours. The set of valid values are defined in subclause 7.3.13.

Table 6.2.1-2: Data Pull Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental_Result (See 7.4)	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Data Management application errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Returned Data	Data (See 7.3.22)	C	This information element shall contain the requested data that is successfully returned. This information element shall be present when all requested data exist in the MCPTT User Database, the requesting entity has permissions to read them and they are all successfully read. Otherwise, it shall be absent.
Failed Requested Data	Data-Identification (See 7.3.3)	C	This information element indicates the requested data that cannot be retrieved by the requesting entity, when the corresponding error only applies to some of the requested data. The set of valid values are defined in 7.3.3. This information element shall be present when the Experimental-Result-Code AVP is set to "DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ" or "DIAMETER_ERROR_UNKNOWN_DATA" and more than one data was requested. Otherwise, it may be absent.
DPA Flags	DPA-Flags (See 7.3.14)	O	This information element contains one or several flags that define different command behaviours. The set of valid values are defined in subclause 7.3.14.

6.2.1.2 Detailed behaviour of the requesting entity

The MCPTT Server or the Configuration Management Server shall make use of this procedure to retrieve from the MCPTT User Database the MCPTT User Profile associated to an MCPTT User. The request shall include the MCPTT ID identifying the MCPTT User and the requested data. The MCPTT Server or the Configuration Management Server may set the "Subscription to notifications" flag in the DPR-Flags to subscribe to the service of notifications for any change for the requested data is requested. Otherwise, the "Subscription to notifications" flag in the DPR-Flags shall be cleared.

The MCPTT Server or the Configuration Management Server may make use of this procedure to unsubscribe to the notifications service for a given MCPTT User. The request shall include the MCPTT ID identifying the MCPTT User. The "Subscription to notifications" flag shall be cleared in the DPR-Flags to unsubscribe to the service of notifications for any change for the requested data.

When receiving the Data Pull response with the Result Code set to "DIAMETER_SUCCESS" with the requested MCPTT User data, the MCPTT Server or the Configuration Management Server should store the received data if the subscription to the notifications service was requested and the "Notifications service status" flag is set by the MCPTT User Database in the DPA-Flags AVP.

6.2.1.3 Detailed behaviour of the MCPTT User Database

The MCPTT User Database may prioritise the received request message according to priority level received within the DRMP AVP.

Upon reception of the Data Pull Request, the MCPTT User Database shall check whether the MCPTT ID for whom data is asked exists in the MCPTT User Database. If not, Experimental-Result-Code shall be set to "DIAMETER_ERROR_USER_UNKNOWN" in the Data Pull Response.

The MCPTT User Database shall check whether the requested data exist. If one or more requested data are not recognized or supported by the MCPTT User Database, the MCPTT User Database shall set the Experimental-Result-Code to "DIAMETER_ERROR_UNKNOWN_DATA" in the Data Pull Response and the Failed Requested Data information element shall be included, indicating the requested data that are not recognized or supported by the MCPTT User Database, if more than one data was requested.

The MCPTT User Database shall check the Requesting Node permissions list (see subclause 6.3) to determine whether the requested data are allowed to be retrieved by the requesting node by checking the combination of the identity of the node sending the request (identified by the Origin-Host AVP included in the request) and the supplied Requested Data. If one or more requested data are not allowed to be retrieved, Experimental-Result-Code shall be set to "DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ" in the Data Pull Response and the Failed Requested Data information element shall be included, indicating the requested data that are not allowed to be read, if more than one data was requested.

The MCPTT User Database shall check whether the requested data are currently being updated by another entity. If there is an update of the data in progress, the MCPTT User Database may delay the Data Pull Response until the update has been completed. The MCPTT User Database shall ensure that the data returned is not corrupted due to the race condition. If the MCPTT User Database is not able to delay the Data Pull Response (e.g. due to timeout), the Experimental-Result-Code shall be set to "DIAMETER_USER_DATA_NOT_AVAILABLE" in the Data Pull Response.

If the "Subscription to notifications" flag in the DPR-Flags was set in the request to subscribe to the service of notifications for any change in the requested data associated with the MCPTT ID, the MCPTT User Database shall check the Requesting Node permissions list (see subclause 6.3) to determine whether the requested data are allowed to be subscribed to notifications by the requesting node by checking the combination of the identity of the node sending the request (identified by the Origin-Host AVP included in the request) and the supplied Requested Data. If one or more requested data are not allowed to be subscribed to notifications, the "Notifications service status" flag in the DPA-Flags AVP in the Data Pull Response shall be clear. Otherwise , the MCPTT User Database shall associate the requesting node identity (identified by the Origin-Host AVP included in the Data Pull Request) with the list of entities that need to be notified when the data requested in the request are modified and the "Notifications service status" flag shall be set in the DPA-Flags AVP in the Data Pull Response.

If the "Subscription to notifications" flag in the DPR-Flags was cleared in the request and a subscription for the data exist in the MCPTT User Database, the MCPTT User Database shall remove the requesting node identity (identified by the Origin-Host AVP included in the Data Pull Request) from the list of entities that need to be notified for the requested data indicated in the request and shall clear the "Notifications service status" flag in the DPA-Flags AVP in the Data Pull Response.

If there is an error in any of the above steps then the MCPTT User Database shall stop processing and shall return the error code specified in the respective step. Or if the MCPTT User Database cannot fulfil the received request for reasons not stated in the above steps, e.g. due to a database error, it shall stop processing the request and set Result-Code to "DIAMETER_UNABLE_TO_COMPLY". Otherwise, the MCPTT User Database shall set the Result-Code to "DIAMETER_SUCCESS" in the Data Pull Response and shall include the requested data.

6.2.2 Data Update

6.2.2.1 General

This procedure is used between the Configuration Management Server and the MCPTT User Database. The procedure is invoked by the Configuration Management Server and is used:

- To update information about a specific MCPTT User stored into the MCPTT User Database.

  NOTE: This procedure cannot be used to create or delete an MCPTT User contained in the MCPTT User Database. An MCPTT User shall be created with at least one MCPTT User Profile.

This procedure is mapped to the commands Data-Update-Request/Answer in the Diameter application specified in the subclause 7.2.5 and 7.2.6. The tables 6.2.2-1 and 6.2.2-2 detail the involved information elements.

Table 6.2.2-1: Data Update Request

Information element name	Mapping to Diameter AVP	Cat.	Description
MCPTT ID	User-Identifier (See 7.3.8)	M	This information element contains the MCPTT ID of the user for whom the data is required. See 3GPP TS 23.179 [2]. See subclause 7.3.8 for the content of this AVP.

Data To Update	Data (See 7.3.22)	M	This information element shall contain the data to be updated.
DUR Flags	DUR-Flags (See 7.3.15)	O	This information element contains one or several flags that define different command behaviours. The set of valid values are defined in subclause 7.3.15.

Table 6.2.2-2: Data Update Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result (See 7.4)	M	Result of the update of data in the MCPTT User Database. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Data Management application errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
MCPTT User Profile Data	MCPTT-User-Profile-Data (See 7.3.20)	C	This information shall contain the User-Data-Id associated with an MCPTT User Profile that has not been successfully updated if more than one MCPTT User Profile is associated with the same MCPTT User. This information may also include the Sequence number associated with this MCPTT User Profile Data. This information element shall be present if data requested to be updated are MCPTT User Profile data and the Result-Code AVP is set to "DIAMETER_LIMITED_SUCCESS" or the Experimental-Result-Code AVP is set to "DIAMETER_ERROR_UNKNOWN_DATA", 'DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED" or "DIAMETER_ERROR_PRIOR_UPDATE_IN_PROGRESS". Otherwise, it shall be absent.
Failed Requested Data	Data-Identification (See 7.3.3)	C	This information element indicates the data that have not been successfully updated. The set of valid values are defined in 7.3.3. This information element shall be present if the Result-Code AVP is set to "DIAMETER_LIMITED_SUCCESS" or the Experimental-Result-Code AVP is set to "DIAMETER_ERROR_UNKNOWN_DATA", 'DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED" or "DIAMETER_ERROR_PRIOR_UPDATE_IN_PROGRESS". Otherwise, it may be absent.
DUA Flags	DUA-Flags (See 7.3.16)	O	This information element contains one or several flags that define different command behaviours. The set of valid values are defined in subclause 7.3.16.

6.2.2.2 Detailed behaviour of the Configuration Management Server

The Configuration Management Server shall make use of this procedure to update data associated to an MCPTT User stored into the MCPTT User Database. The request shall include the MCPTT ID identifying the MCPTT User and the data requested to be updated.

When data requested to be updated are the MCPTT User Profile data, the request shall include the MCPTT User Profile data and the Sequence Number associated with the MCPTT User Profile. The request may also include the User Data Id if more than one MCPTT User Profile is associated with the same MCPTT User. Multiple MCPTT User Profiles can be updated and, in this case, each MCPTT User Profile data shall contain a Sequence Number and the User Data Id. Each updated MCPTT User Profile data shall be associated with a Sequence Number of n+1 where n is the original Sequence Number associated with the MCPTT User Profile before modification. If n was equal to 65535, the new associated Sequence Number shall be equal to 1.

When more than one data is requested to be updated, the Configuration Management Server may set the "Atomicity" flag in the DUR-Flags to indicate that all the requested data shall be updated by the MCPTT User Database or none of them shall be updated if at least one data element cannot be updated.

When receiving "DIAMETER_LIMITED_SUCCESS" in the Data Update Response, including the indication of the requested data that have not been successfully updated, the Configuration Management Server may reattempt to update the affected data.

When receiving "DIAMETER_ERROR_DATA_OUT_OF_SYNC" in the Data Update Response when attempting to update an MCPTT User Profile, the Configuration Management Server may attempt to resolve the inconsistency between the version of the MCPTT User Profile that it holds and the version stored at the MCPTT User Database. It may execute a Data Pull to retrieve the current version of the data from the MCPTT User Database or it may wait to receive a subsequent Notification request from the MCPTT User Database for the affected MCPTT User Profile.

When receiving "DIAMETER_ERROR_PRIOR_UPDATE_IN_PROGRESS" in the Data Update Response, the configuration Management Server may wait to receive a subsequent Notification request from the MCPTT User Database for the affected MCPTT User Profile or it may reattempt to update the data.

6.2.2.3 Detailed behaviour of the MCPTT User Database

The MCPTT User Database may prioritise the received request message according to priority level received within the DRMP AVP.

Upon reception of the Data Update Request, the MCPTT User Database shall check whether the MCPTT ID for whom data is asked exists in the MCPTT User Database. If not, Experimental-Result-Code shall be set to "DIAMETER_ERROR_USER_UNKNOWN" in the Data Update Response.

The MCPTT User Database shall check whether the requested data exist. If any of the requested data is not available into the MCPTT User Database, the MCPTT User Database shall set the Experimental-Result-Code to "DIAMETER_ERROR_UNKNOWN_DATA" in the Data Update Response and the Failed Requested Data information element shall be included, indicating the requested data that are unknown to the MCPTT User Database, if more than one data was requested.

The MCPTT User Database shall check the Requesting Node permissions list (see subclause 6.3) to determine whether the requested user data is allowed to be updated by this requesting node by checking the combination of the identity of the node sending the request (identified by the Origin-Host AVP included in the request) and the supplied Requested Data. If any of the requested data is not allowed to be updated, Experimental-Result-Code shall be set to "DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED" in the Data Update Response and the Failed Requested Data information element shall be included, indicating the requested data that are not allowed to be modified, if more than one data was requested.

The MCPTT User Database shall check whether the data that is requested to be updated by the requesting node is currently being updated by another entity. If there is an update of any requested data in progress, Experimental-Result-Code shall be set to "DIAMETER_ERROR_PRIOR_UPDATE_IN_PROGRESS" in the Data Update Response and the Failed Requested Data information element shall be included, indicating the requested data that are being updated by another entity, if more than one data was requested.

If the updated data are MCPTT User Profile data, the MCPTT User Database shall identify the MCPTT User Profile to update using the User Data Id (if multiple MCPTT User Profiles exist) and check the Sequence Number contained in the MCPTT User Profile data included in the request. If either:

- the Sequence Number is equal to 0;

- or (Sequence_Number_in_Data_Update - 1) is not equal to (Sequence_Number_In_MCPTT_User_Database modulo 65535);

then, the Experimental-Result-Code shall be set to "DIAMETER_ERROR_DATA_OUT_OF_SYNC" in the Data Update Response.

If there is more data than the MCPTT User Database is prepared to accept then Experimental-Result-Code shall be set to "DIAMETER_ERROR_TOO_MUCH_DATA" and the new data shall be discarded.

If the data requested to be updated are the MCPTT User Profile data and if the MCPTT User Profile and/or the Sequence Number and/or the User Data Id (if multiple MCPTT User Profiles exist) is not present in the request, then Experimental-Result-Code shall be set to "DIAMETER_ERROR_REQUIRED_KEY_NOT_PROVIDED", the Failed Requested Data information element shall be included indicating the requested data that causes the error (if more than one data was requested) and the operation shall be ignored by the MCPTT User Database.

If multiple data have to be updated, the steps above shall be repeated for each data element. The MCPTT User Database shall check if the "Atomicity" flag in set in the DUR-Flags:

- If set and the MCPTT User Database does not support atomic operation, the MCPTT User Database shall set the Result-Code to "DIAMETER_ERROR_ATOMICITY_NOT_SUPPORTED" in the Data Update Response and no data shall be updated.

- If set and the MCPTT supports atomic update operation, if one of the updates fails, the MCPTT User Database shall keep or restore all the stored data as they were before receiving the Data Update request and the MCPTT User Database shall send the Data Update Response with the Result-Code or Experimental-Result set to value appropriate to the encountered error case. Otherwise, if all updated are successful, the requested operation shall take place and the MCPTT User Database shall return the Result-Code AVP set to "DIAMETER_SUCCESS" in the Data Update Response

- If not set, the Data Update may be partially successful if it is successful for the update of only a part of the data instances in the request. In such a case, the MCPTT User Database shall set the Result-Code to "DIAMETER_LIMITED_SUCCESS" in the Data Update Response. This Data Update Response indicates the data that have not been successfully updated. If the requested update was for more than one MCPTT User Profile, the MCPTT User Database shall include in the Data Update Response the User-Data-Id of the MCPTT User Profile(s) that has/have not been successfully updated.

The successfully updated data stored at the MCPTT User Database shall trigger the sending of notifications to any other entities that are subscribed to Notifications for updates to the modified data for that MCPTT ID (see 6.2.3).

If the updated data are MCPTT User Profile, the Sequence Number received in the Data Update request shall be associated with the updated MCPTT User Profile data, optionally identified by the User-Data-Id in the request.

If there is an error in any of the above steps then the MCPTT User Database shall stop processing and shall return the error code specified in the respective step (see subclause 7.4 for an explanation of the error codes).

If the MCPTT User Database cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to "DIAMETER_UNABLE_TO_COMPLY" in the Data Update Response.

6.2.3 Data Notification

6.2.3.1 General

This procedure is used between the MCPTT User Database and the MCPTT Server or the Configuration Management Server. The procedure is invoked by the MCPTT User Database and is used:

- To inform the MCPTT Server or the Configuration Management Server of changes in particular information associated with an MCPTT ID stored in the MCPTT User Database to which the MCPTT Server or the Configuration Management Server has previously subscribed to receive Notifications for, using the Data Pull request (see 6.2.1).

This procedure is mapped to the commands Notification-Data-Request/Answer in the Diameter application specified in the subclause 7.2.7 and 7.2.8. The tables 6.2.3-1 and 6.2.3-2 detail the involved information elements.

Table 6.2.3-1: Data Notification Request

Information element name	Mapping to Diameter AVP	Cat.	Description
MCPTT ID	User-Identifier (See 7.3.8)	M	This information element contains the MCPTT ID of the user for whom the data is required. See 3GPP TS 23.179 [2]. See subclause 7.3.8 for the content of this AVP.
Returned Data	Data (See 7.3.22)	M	This information element shall contain the data to which the requesting entity is subscribed to notification of change.
NDR Flags	NDR-Flags (See 7.3.17)	O	This information element contains one or several flags that define different command behaviours. The set of valid values are defined in subclause 7.3.13.

Table 6.2.3-2: Data Notification Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result (See 7.4)	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Data Management application errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Failed Requested Data	Data-Identification (See 7.3.3)	C	This information element indicates the requested information that the receiving entity is not able to process. The set of valid values are defined in 7.3.3. This information element shall be present when the Experimental-Result-Code AVP is set to "DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA", or "DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED". Otherwise, it may be absent.
NDA Flags	NDA-Flags (See 7.3.18)	O	This information element contains one or several flags that define different command behaviours. The set of valid values are defined in subclause 7.3.18.

6.2.3.2 Detailed behaviour of the MCPTT User Database

The MCPTT User Database shall make use of this procedure to update information associated with an MCPTT User for which a MCPTT Server or a Configuration Management Server has previously subscribed to receive Notifications for. The request shall include the MCPTT Identity identifying the MCPTT User and the modified data.

If the notification is sent to modify an MCPTT User Profile, the request shall include the MCPTT User Profile data, including the Sequence number and the User Data Id (required if more than one MCPTT User Profile exists).

When receiving the Notification response with the Experimental-Result-Code set to "DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA", "DIAMETER_ERROR_USER_UNKNOWN", "DIAMETER_ERROR_TOO_MUCH_DATA" or "DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED", the

MCPTT User Database shall remove the responding entity from the list of entities that need to be notified of any change in information associated with the MCPTT ID included in the request.

6.2.3.3 Detailed behaviour of the receiving entity

The MCPTT Server or the Configuration Management Server may prioritise the received request message according to priority level received within the DRMP AVP.

Upon reception of the Notification Request, the receiving entity shall check whether the MCPTT ID for which the Notification Request is received is served by the receiving entity. If not, the Experimental-Result-Code shall be set to "DIAMETER_ERROR_USER_UNKNOWN" in the Notification Data Response.

The receiving entity shall check whether the modified data are recognized or supported by the receiving entity. If not, the Experimental-Result-Code shall be set to "DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED" in the Notification Response. This Notification Data Response shall indicate the data that are not recognized or supported by the receiving entity, if more than one data was requested.

The receiving entity shall check whether it has subscribed to notifications for the modified data that are received. If not, the Experimental-Result-Code shall be set to "DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA" in the Notification Data Response. This Notification Data Response shall indicate the data for which the notification service has not been subscribed, if more than one data was requested.

If there is more data than the receiving entity is prepared to accept then Experimental-Result-Code shall be set to "DIAMETER_ERROR_TOO_MUCH_DATA" and the new data shall be discarded. This Notification Data Response may indicate the data that have not been successfully updated

If the notification includes multiple data that are modified, the steps above shall be repeated for each data element. If an error occurs, the receiving entity shall stop processing and shall return the Result-Code or Experimental-Result-Code set to value specified in the respective step (see subclause 7.4 for an explanation of the error codes). The Notification Data Response may indicate the requested data that have not been successfully processed.

Otherwise, the requested operation shall take place and the receiving entity shall return the Result-Code AVP set to "DIAMETER_SUCCESS" in the Notification Response. If the receiving entity locally stores the data for which it has received the notification, the received data shall be updated. In this case, if the modified data are MCPTT User Profile data, each modified MCPTT User Profile shall be associated with the corresponding Sequence Number received in the Notification request.

6.3 Requesting entity permissions list

6.3.1 General

Some of the individual elements identified by the Requested-Data AVP may be requested by the MCPTT Server or the Configuration Management Server from the MCPTT User Database using the Data Pull operation (see subclause 6.2.1) or may be updated at the MCPTT User Database by the Configuration Management Server using the Data Update operation (see subclause 6.2.2). The MCPTT Server or the Configuration Management Server may also request the MCPTT User Database to be notified of changes to specific elements identified by Requested-Data AVP using the "Subscription to notifications" flag in the DPR-Flags of the Data Pull operation (see subclause 6.2.1). The MCPTT User Database will only allow these operations to take place if the requested data element is permitted to be included in the specific command requested by the MCPTT Server or the Configuration Management Server.

To manage whether an MCPTT Server or a Configuration Management Server may request each requested data element with a specific operation, the MCPTT User Database shall maintain a list of Requesting Entity permissions (the "Requesting Entity Permissions List"). Requesting entity permissions are identified by the requesting entity identity and the Requested Data with the possible permissions associated with each requested Data for Data Pull and Data Update operations or any combination of these permissions. The permissions shall apply to all users served by the MCPTT User Database. When an MCPTT Server or a Configuration Management Server requests Data Pull or Data Update, the MCPTT User Database shall check permissions and return an error result if the MCPTT Server or the Configuration Management Server does not have the required permission. If the Requesting Entity permissions change in a later stage, the MCPTT User Database shall update the "Requesting Entity Permission List" accordingly.

Table 6.3-1 defines the requested data, access key and requesting entity permissions for the operation(s) on data accessible via the MCPTT-2 or CSC-13 interface, i.e. the listed operation(s) in the Operations column are the only ones allowed to be used with this Requested Data value. It is a matter of operator policy to further restrict the requesting entity permission rights defined in table 6.3-1.

An access key between square brackets is considered as optional, while when more than one access key is separated by logical OR and included between brackets, it means that one (and only one) of these access keys is mandatory.

Table 6.3.1-1: Data accessible via MCPTT-2 or CSC-13 interface

Bit.	Data element	Defined in	Access key	Operations
0	MCPTT User Profile	7.3.3	Requested Data + MCPTT ID	Data Pull (Read) Data Pull (Subscription to Notification)
			MCPTT ID	Data Update (NOTE 1)
NOTE 1: In this release, Data update operations are only allowed for Configuration Management Servers				

7 Protocol Specification and Implementation for MCPTT

7.1 General

7.1.1 Use of Diameter base protocol

The Diameter Base Protocol as specified in IETF RFC 3588 [3] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and error codes as specified in this specification. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) shall be used unmodified.

7.1.2 Securing Diameter Messages

For secure transport of Diameter messages, see 3GPP TS 33.210 [4].

7.1.3 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the MCPTT-2 and CSC-13 interfaces.

7.1.4 Use of sessions

Between the MCPTT Server and the MCPTT User Database or between the Configuration Management Server and the MCPTT User Database, Diameter sessions shall be implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client shall not send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 3588 [3]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

7.1.5 Transport protocol

Diameter messages over the MCPTT-2 and CSC-13 interfaces shall make use of SCTP IETF RFC 4960 [5].

7.1.6 Routing considerations

This subclause specifies the use of the Diameter routing AVPs Destination-Realm and Destination-Host.

The Destination-Realm AVP shall contain the network domain name of the MCPTT service provider's domain. The network domain name is either known by the sending MCPTT Server or the Configuration Management Server or is derived from information received at the signalling layer.

If an MCPTT Server or the Configuration Management Server knows the address/name of the MCPTT User Database in charge of a given MCPTT User, both the Destination-Realm and Destination-Host AVPs shall be present in the request.

If an MCPTT Server or the Configuration Management Server knows only the network domain name, the Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node. When multiple and separately addressable MCPTT User Databases have been deployed by the MCPTT service provider/network operator, the next Diameter node is either a Diameter Proxy Agent or a Diameter Redirect Agent responsible for the determination of the destination MCPTT User Database (as described in subclause 7.1.10). When the next Diameter node is a Diameter Agent Proxy, the Diameter Proxy Agent, based on the result of this determination, shall modify the Destination-Realm AVP and Destination-Host AVP of the request appropriately. The Diameter Proxy Agent shall then append a Route-Record AVP to the request and shall send the request to the destination MCPTT User Database. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by an MCPTT User Database.

When the response is routed back to a Diameter Proxy Agent, the Diameter Proxy Agent shall send the response back to the MCPTT Server or the Configuration Management Server without modifying the Origin-Realm AVP and Origin-Host AVP. The response shall contain the Origin-Realm AVP set to the realm and the Origin-Host AVP set to the FQDN of the MCPTT User Database that have sent the response. The MCPTT Server shall then store the MCPTT User Database realm and identity for each MCPTT ID for sending further requests for the same MCPTT User.

Requests initiated by the MCPTT User Database towards an MCPTT Server shall include both Destination-Host and Destination-Realm AVPs. The MCPTT User Database obtains the Destination-Host AVP to use in requests towards an MCPTT Server or the Configuration Management Server, from the Origin-Host AVP received in previous requests from the MCPTT Server or the Configuration Management Server.

Consequently, the Destination-Realm AVP and Destination-Host AVP are declared as mandatory in the ABNF for all requests initiated by the MCPTT User Database.

Consequently, the Destination-Realm AVP is declared as mandatory and the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by a MCPTT Server.

If the Vendor-Specific-Application-ID AVP is received in any of the commands, it may be ignored by the receiving node, and it shall not be used for routing purposes.

NOTE: The Vendor-Specific-Application-ID can be included as an optional AVP in all commands in order to ensure interoperability with diameter agents following a strict implementation of IETF RFC 3588 [3], by which messages not including this AVP will be rejected. IETF RFC 3588 [7] indicates that the AVP is present in all proxiable commands, such as those defined in this specification, despite the fact that the contents of this AVP are redundant since the Application ID is already present in the command header. This AVP can be removed in subsequent revisions of this specification, once the new diameter base protocol specification will be adopted by 3GPP.

7.1.7 Advertising Application Support

The MCPTT User Database and the MCPTT Server or the Configuration Management Server shall advertise support of the Diameter Data Management Application by including the value of the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The vendor identifier value of 3GPP (10415) shall be included in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and in the Vendor-Id AVP within the Vendor-

Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per IETF RFC 3588 [3].

7.1.8 Diameter Application Identifier

The Diameter Data Management application protocol shall be defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

The Diameter application identifier assigned to the Diameter Data Management application is 16777351 (allocated by IANA).

7.1.9 Use of the Supported-Features AVP

When new functionality is introduced on the MCPTT-2 or CSC-13 interfaces, it should be defined as optional. If backwards incompatible changes cannot be avoided, the new functionality shall be introduced as a new feature and support advertised with the Supported-Features AVP. The usage of the Supported-Features AVP on the MCPTT-2 and CSC-13 interfaces is consistent with the procedures for the dynamic discovery of supported features as defined in subclause 7.2 of 3GPP TS 29.229 [6].

When extending the application by adding new AVPs for a feature, the new AVPs shall have the M bit cleared and the AVP shall not be defined mandatory in the command ABNF.

As defined in 3GPP TS 29.229 [6], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the all reference points as specified in this specification, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

7.1.10 MCPTT ID to MCPTT User Database resolution

The MCPTT ID to MCPTT User Database resolution mechanism enables the MCPTT Server or the Configuration Management Server to find the identity of the MCPTT User Database that holds the MCPTT related data for a given MCPTT ID when multiple and separately addressable MCPTT User Databases have been deployed by the MCPTT service provider/network operator. The resolution mechanism is not required in networks that utilise a single MCPTT User Database or when an MCPTT Server is configured to use pre-defined MCPTT User Database.

The resolution mechanism shall use a Diameter Proxy Agent or a Diameter Redirect Agent.

The Diameter Proxy Agent or Diameter Redirect Agent shall be used to determine the MCPTT User Database identity.

In networks where the use of the MCPTT ID to MCPTT User Database resolution mechanism is required and the MCPTT Server is not configured to use a predefined MCPTT User Database, each MCPTT Server shall be configured with the pre-configured address/name of a Diameter Proxy Agent or Diameter Redirect Agent to enable use of these resolution mechanisms.

To get the MCPTT User Database identity, the MCPTT Server or the Configuration Management Server shall send the Data Management Application request normally destined to the MCPTT User Database to the pre-configured Diameter Proxy Agent or Diameter Redirect Agent.

The Diameter Proxy Agent shall determine the MCPTT User Database identity and shall forward the Data Management Application request directly to the MCPTT User Database. The MCPTT Server shall determine the MCPTT User Database identity from the response to the Data Management Application request received from the MCPTT User Database. The MCPTT Server and the Configuration Management Server should store the MCPTT User Database identity/name/Realm and shall use it in further Data Management Application requests associated to the same MCPTT ID.

The Diameter Redirect Agent shall determine the MCPTT User Database address and shall send to the MCPTT Server or the Configuration Management Server a notification of redirection towards the MCPTT User Database, in response to the request. Multiple MCPTT User Database identities may be included in the response, as specified in IETF RFC 3588 [9]. In such a case, the MCPTT Server or the Configuration Management Server shall send the Request to the first MCPTT User Database identity in the ordered list received in the Response from the Diameter Redirect Agent. If the MCPTT Server or the Configuration Management Server does not receive a successful response to the Request, the MCPTT Server or the Configuration Management Server shall send a Request to the next MCPTT User Database identity in the ordered list. This procedure shall be repeated until a successful response from an MCPTT User Database is received.

7.2 Commands

7.2.1 Introduction

This subclause defines the Command code values and related ABNF for each command described in this specification.

7.2.2 Command-Code values

This subclause defines Command-Code values for the Diameter Data Management application used over the MCPTT-2 and CSC-13 interfaces as allocated by IANA.

Every command is defined by means of the ABNF syntax IETF RFC 5234 [7], according to the rules in IETF RFC 3588 [3]. In the case, the definition and use of an AVP is not specified in this document, the guidelines in IETF RFC 3588 [3] shall apply.

NOTE: For this release, the Vendor-Specific-Application-ID is included as an optional AVP in all commands in order to ensure interoperability with diameter agents following a strict implementation of IETF RFC 3588 [3], by which messages not including this AVP will be rejected. IETF RFC 3588 [3] indicates that the AVP shall be present in all proxiable commands, such as those specified here, despite that the contents of this AVP are redundant since the Application ID is already present in the command header. This AVP may be removed in subsequent revisions of this specification, once the diameter base protocol is updated accordingly.

The following Command Codes are defined in this specification:

Table 7.2.2-1: Command-Code values

Command-Name	Abbreviation	Code	Section
Data-Pull-Request	DPR	8388728	7.2.3
Data-Pull-Answer	DPA	8388728	7.2.4
Data-Update-Request	DUR	8388729	7.2.5
Data-Update-Answer	DUA	8388729	7.2.6
Notification-Data-Request	NDR	8388730	7.2.7
notification-Data-Answer	NDA	8388730	7.2.8

7.2.3 Data-Pull-Request (DPR) Command

The Data-Pull-Request (DPR) command, indicated by the Command-Code field set to 8388728 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request user data.

Message Format

```
< Data-Pull-Request > ::=   < Diameter Header: 8388728, REQ, PXY, 16777351 >
                                < Session-Id >
                                [ DRMP ]
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              [ Destination-Host ]
                              { Destination-Realm }
                              *[ Supported-Features ]
                              [ User-Identifier ]
                              *[ Data-Identification ]
                              [ DPR-Flags ]
                              [ OC-Supported-Features ]
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

7.2.4 Data-Pull-Answer (DPA) Command

The Data-Pull-Answer (DPA) command, indicated by the Command-Code field set to 8388728 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Data-Pull-Request command. The Experimental-Result AVP may contain one of the values defined in subclause 7.4.

Message Format

```
< Data-Pull-Answer > ::=    < Diameter Header: 8388728, PXY, 16777351 >
                              < Session-Id >
                              [ DRMP ]
                              [ Result-Code ]
                              [ Experimental-Result ]
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              *[ Supported-Features ]
                              *[ Data ]
                              *[ Data-Identification ]
                              [ DPA-Flags]
                              [ OC-Supported-Features ]
                              [ OC-OLR ]
                              *[ AVP ]
                              [ Failed-AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

7.2.5 Data-Update-Request (DUR) Command

The Data-Update-Request (DUR) command, indicated by the Command-Code field set to 8388729 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to update user data in the server.

Message Format

```
< Data-Update-Request > ::=    < Diameter Header: 8388729, REQ, PXY, 16777351 >
                                 < Session-Id >
                                 [ DRMP ]
                                 { Auth-Session-State }
                                 { Origin-Host }
                                 { Origin-Realm }
                                 [ Destination-Host ]
                                 { Destination-Realm }
                                 *[ Supported-Features ]
                                 [ User-Identifier ]
                                 [ Data ]
                                 [ DUR-Flags ]
                                 [ OC-Supported-Features ]
                                 *[ AVP ]
                                 *[ Proxy-Info ]
                                 *[ Route-Record ]
```

7.2.6 Data-Update-Answer (DUA) Command

The Data-Update-Answer (DUA) command, indicated by the Command-Code field set to 8388729 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Data-Update-Request command. The Experimental-Result AVP may contain one of the values defined in subclause 7.4.

Message Format

```
< Data-Update-Answer > ::=< Diameter Header: 8388729, PXY, 16777351 >
                             < Session-Id >
                             [ DRMP ]
```

[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[Data-Identification]
*[MCPTT-User-Profile-Data]
[DUA-Flags]
*[Supported-Features]
[OC-Supported-Features]
[OC-OLR]
*[AVP]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.2.7 Notification-Data-Request (PDR) Command

The Notification-Data-Request (PDR) command, indicated by the Command-Code field set to 8388730 and the 'R' bit set in the Command Flags field, is sent by a Diameter server to a Diameter client in order to notify changes in the user data stored in the server.

Message Format

< Notification-Data-Request > ::= < Diameter Header: 8388730, REQ, PXY, 16777351 >
< Session-Id >
[DRMP]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
*[Supported-Features]
[User-Identifier]
[Data]
[NDR-Flags]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.2.8 Notification-Data-Answer (PDA) Command

The Notification-Data-Answer (PDA) command, indicated by the Command-Code field set to 8388730 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Push-Data-Request command. The Experimental-Result AVP may contain one of the values defined in subclause 7.4.

Message Format

< Notification-Data-Answer > ::=< Diameter Header: 8388730, PXY, 16777351 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[Data-Identification]
[NDA-Flags]
*[Supported-Features]
*[AVP]
[Failed-AVP]

*[Proxy-Info]
*[Route-Record]

7.3 AVPs

7.3.1 General

The following table (table 7.3.1-1) specifies the Diameter AVPs defined for the MCPTT-2 and CSC-13 interfaces, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-ID header of all AVPs defined in this specification shall be set to 3GPP (10415).

For all AVPs which contain bit masks and are of the type Unsigned32 e.g., DPR-Flags, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x0001 shall be used.

Table 7.3.1-1: MCPTT-2 and CSC-13 specific Diameter AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
MCPTT-ID	4500	7.3.2	UTF8String	M, V				No
Data-Identification	4501	7.3.3	Grouped	M, V				No
Data-Identification-Prefix	4502	7.3.11	Unsigned32	M,V				No
Data-Identification-Flags	4503	7.3.12	Unsigned64	M,V				No
DPR-Flags	4504	7.3.13	Unsigned32	M,V				No
DPA-Flags	4505	7.3.14	Unsigned32	M,V				No
DUR-Flags	4506	7.3.15	Unsigned32	M,V				No
DUA-Flags	4507	7.3.16	Unsigned32	M,V				No
NDR-Flags	4508	7.3.17	Unsigned32	M,V				No
NDA-Flags	4509	7.3.18	Unsigned32	M,V				No
User-Data-Id	4510	7.3.19	Unsigned32	M,V				No
MCPTT-User-Profile-Data	4511	7.3.20	Grouped	M,V				No
Sequence-Number	4512	7.3.21	Unsigned32	M,V				No
Data	4513	7.3.22	Grouped	M,V				No
NOTE 1: The AVP header bit denoted as "M", indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [3].								
NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.								

The following table (table 7.3.1-2) specifies the Diameter AVPs re-used by the MCPTT-2 and CSC-13 interfaces from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within MCPTT-2 and CSC-13 interfaces.

Any other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported. The AVPs from Diameter Base Protocol are not included in table 7.3.1-2.

Table 7.3.1-2: MCPTT-2 and CSC-13 re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
Supported-Features	3GPP TS 29.229 [6]		
DRMP	IETF draft-ietf-drmp-03 [8]		Must set
Feature-List-ID	3GPP TS 29.229 [6]		
Feature-List	3GPP TS 29.229 [6]	See subclause 7.3.10	
Feature-Id	3GPP TS 29.229 [6]		
User-Data	3GPP TS 29.329 [9]		
User-Identifier	3GPP TS 29.336 [10]	See subclause 7.3.8	
OC-Supported-Features	IETF RFC 7683 [11]	See subclause 7.3.6	Must set
OC-OLR	IETF RFC 7683 [11]	See subclause 7.3.5	Must set
NOTE 1: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.			

7.3.2 MCPTT-ID

The MCPTT-ID AVP is of type UTF8String, and it shall contain an URI as defined in IETF RFC 3986 [15].. For more information see 3GPP TS 23.179 [2].

7.3.3 Requested-Data

The Data-Identification AVP is of type Grouped. It shall contain the Data-Identification-Prefix AVP and the Data-Identification-Flags AVP. AVP format

Data-Identification ::= < AVP header: 4501 10415 >

{ Data-Identification-Prefix}

{ Data-Identification-Flags }

*[AVP]

7.3.4 DRMP

The DRMP AVP is of type Enumerated and it is defined in IETF draft-ietf-dime-drmp-03 [8]. This AVP allows the MCPTT User Database and the MCPTT Server to indicate the relative priority of Diameter messages.

7.3.5 OC-OLR

The OC-OLR AVP is of type Grouped and it is defined in IETF RFC 7683 [11]. This AVP is used to support Diameter overload control mechanism.

7.3.6 OC-Supported-Features

The OC-Supported-Features AVP is of type Grouped and it is defined in IETF RFC 7683 [11]. This AVP is used to support Diameter overload control mechanism.

7.3.7 User-Data

The User-Data AVP is of type OctetString and it contains an XML document. This AVP is defined in the 3GPP TS 29.329 [9].

When the requested data managed by the MCPTT User Database is an MCPTT User Profile, this AVP contains an XML document conformant to the XML schema defined in subclause 7.4 in the 3GPP TS 24.384 [16]. This XML schema describes the MCPTT User Profile data exchanged between the MCPTT User Database and the MCPTT Server

in the DPR/DPA and NDR/NDA and between the MCPTT User Database and the Configuration Management Server in DPR/DPA, NDR/NDA and DUR/DUA operations.

7.3.8 User-Identifier

The User-Identifier AVP is of type Grouped. It shall contain the identifier used to identify the MCPTT User in the MCPTT User Database. This AVP is defined in the 3GPP TS 29.336 [10] and is extended to contain an MCPTT ID.

AVP format:

User-Identifier ::= <AVP header: 3102 10415>

[MCPTT-ID]

*[AVP]

Note: In this release, only an MCPTT ID is used to identify an MCPTT User.

7.3.9 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [10]. For this release, the Feature-List-ID AVP value shall be set to 1.

7.3.10 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [6]. A null value indicates that there is no feature used by the application.

NOTE: There is no feature defined for this release.

7.3.11 Data-Identification-Prefix

The Data-Identification-Prefix AVP is of type Unsigned32 and identifies a unique set of data identification flags, in order to ensure further extensibility when all Data-Identification-Flags are assigned.

Each Data-Identification-Flags defined is assigned a unique Data-Identification-Prefix AVP value.

7.3.12 Data-Identification-Flags

The Data-Identification-Flags AVP is of type Unsigned64 and it contains a bit mask.

The meaning of the bits when the Data-Identification-Prefix value is 1 is defined in table 7.3.12-1:

Table 7.3.12-1: Data-Identification-Flags

bit	name	Description
0	MCPTT User Profile	This bit, when set, indicates that the requested data are MCPTT User Profile data.
NOTE:	Bits not defined in this table shall be cleared by the sending entity and discarded by the receiving entity.	

7.3.13 DPR-Flags

The DPR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.13-1:

Table 7.3.13-1: DPR-Flags

Bit	Name	Description
0	Subscription to notifications	This bit, when set, indicates that the requesting node subscribes to the notifications service for any change in the requested data.
NOTE:	Bits not defined in this table shall be cleared by the sending entity and discarded by the receiving entity.	

7.3.14 DPA-Flags

The DPA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.14-1:

Table 7.3.14-1: DPA-Flags

Bit	Name	Description
0	Notification service status	This bit, when set, indicates that the service of notifications is active.
NOTE:	Bits not defined in this table shall be cleared by the sending entity and discarded by the receiving entity.	

7.3.15 DUR-Flags

The DUR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.15-1:

Table 7.3.15-1: DUR-Flags

Bit	Name	Description
0	Atomicity	This bit, when set, indicates that atomicity is required for operations on multiple data.
NOTE:	Bits not defined in this table shall be cleared by the sending entity and discarded by the receiving entity.	

7.3.16 DUA-Flags

The DUA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.16-1:

Table 7.3.16-1: DUA-Flags

Bit	Name	Description
0		
NOTE:	Bits not defined in this table shall be cleared by the sending entity and discarded by the receiving entity.	

NOTE: There is no bit defined for this release.

7.3.17 NDR-Flags

The NDR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.17-1:

Table 7.3.17-1: NDR-Flags

Bit	Name	Description
0		
NOTE:	Bits not defined in this table shall be cleared by the sending entity and discarded by the receiving entity.	

NOTE: There is no bit defined for this release.

7.3.18 NDA-Flags

The NDA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.18-1:

Table 7.3.18-1: NDA-Flags

Bit	Name	Description
0		
NOTE:	Bits not defined in this table shall be cleared by the sending entity and discarded by the receiving entity.	

NOTE: There is no bit defined for this release.

7.3.19 User-Data-Id

The User-Data-Id AVP is of type Unsigned32 and it shall contain the unique identifier of a given MCPTT User Profile defined for an MCPTT User.

7.3.20 MCPTT-User-Profile-Data

The MCPTT-User-Profile-Data AVP is of type Grouped. It may contain an MCPTT User Profile data, a Sequence Number and a User Data Id identifying a specific XML document.

AVP format:

MCPTT-User-Profile-Data ::= <AVP header: 4511 10415>

[User-Data]

[Sequence-Number]

[User-Data-Id]

*[AVP]

7.3.21 Sequence-Number

The Sequence-Number AVP is of type Unsigned32. This AVP contains a number associated to an MCPTT User Profile. This AVP is defined in the 3GPP TS 29.329 [9].

7.3.22 Data

The Data AVP is of type Grouped. It contains one or several AVPs containing the data to be returned.

AVP format:

Data ::= <AVP header: 4513 10415>

* [MCPTT-User-Profile-Data]

*[AVP]

7.4 Result-Code and Experimental-Result-Code Values

7.4.1 Introduction

This subclause defines Result-Code and Experimental-Result-Code values that shall be supported by all Diameter implementations that conform to this specification.

7.4.2 Success

7.4.2.1 General

Result codes that fall within the Success category shall be used to inform a peer that a request has been successfully completed. The Result-Code AVP values defined in Diameter Base Protocol IETF RFC 3588 [3] shall be applied.

7.4.3 Permanent Failures

7.4.3.1 General

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request has failed, and should not be attempted again. The Result-Code AVP values defined in Diameter Base Protocol IETF RFC 3588 [3] shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result-Code AVP and the Result-Code AVP shall be absent.

7.4.3.2 DIAMETER_ERROR_USER_UNKNOWN (5001)

This result code shall be sent by the MCPTT User Database to indicate that the MCPTT User identified by the User Identifier received in the request is unknown. This error code is defined in 3GPP TS 29.229 [6].

7.4.3.3 DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED (5100)

The data received by the MCPTT Server or the Configuration Management Server is not supported or recognized. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.4 DIAMETER_ERROR_OPERATION_NOT_ALLOWED (5101)

The requested operation is not allowed for the user. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.5 DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ (5102)

The requested user data is not allowed to be read. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.6 DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED (5103)

The requested user data is not allowed to be modified. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.7 DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED (5104)

The requested user data is not allowed to be notified on changes. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.8 DIAMETER_ERROR_TOO_MUCH_DATA (5008)

The size of the data pushed to the receiving entity exceeds its capacity. This error code is defined in 3GPP TS 29.229 [6].

7.4.3.9 DIAMETER_ERROR_DATA OUT_OF_SYNC (5105)

The request to update the user profile at the MCPTT User Database could not be completed because the requested update is based on an out-of-date version of the user profile i.e. the Sequence Number in the Data Update Request message does not match with the immediate successor of the associated Sequence Number stored for that user profile at the MCPTT User Database. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.10 DIAMETER_ERROR_FEATURE_UNSUPPORTED (5011)

A request application message was received indicating that the origin host requests that the command pair would be handled using a feature which is not supported by the destination host. This error code is defined in 3GPP TS 29.229 [6].

7.4.2.11 DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA (5107)

The MCPTT Server received a notification of changes of some information to which it is not subscribed. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.12 DIAMETER_ERROR_ UNKNOWN _DATA (5670)

The requested data received by the MCPTT User Database does not exist.

7.4.3.13 DIAMETER_ERROR_REQUIRED_KEY_NOT_PROVIDED (5671)

One or more access keys are missing in the request to be able to update the requested data.

7.4.4 Transient Failures

7.4.4.1 General

Errors that fall within the transient failures category are those used to inform a peer that the request could not be satisfied at the time that it was received. The request may be able to be satisfied in the future.

7.4.3.2 DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

The requested user data is not available at this time to satisfy the requested operation. This error code is defined in 3GPP TS 29.329 [9].

7.4.3.3 DIAMETER_PRIOR_UPDATE_IN_PROGRESS (4101)

The request to update the repository data at the MCPTT User Database could not be completed because the related repository data is currently being updated by another entity. This error code is defined in 3GPP TS 29.329 [9].

Annex A (normative): Diameter overload control mechanism

A.1 General

Diameter overload control mechanism is an optional feature.

IETF RFC 7683 [11] specifies a Diameter overload control mechanism which includes the definition and the transfer of related AVPs between Diameter nodes.

It is recommended to make use of IETF RFC 7683 [11] on the MCPTT-2 and CSC-13 interfaces where, when applied, the MCPTT Server and the Configuration Management Server shall behave as a reacting node and the MCPTT User Database as a reporting node.

Depending on regional/national requirements and network operator policy, priority traffic (e.g. MCPTT emergency call) shall be exempted from throttling due to Diameter overload control up to the point where requested traffic reduction cannot be achieved without throttling the priority traffic.

A.2 MCPTT User Database behaviour

The MCPTT User Database requests traffic reduction from the MCPTT Server when the MCPTT User Database is in an overload situation, including OC-OLR AVP in answer commands as described in IETF RFC 7683 [11].

The MCPTT User Database identifies that it is in an overload situation by implementation specific means. For example, the MCPTT User Database may take into account the traffic over the MCPTT-2 interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources, etc.

The MCPTT User Database determines the specific contents of OC-OLR AVP in overload reports and the MCPTT User Database decides when to send OC-OLR AVPs by implementation specific means.

A.3 MCPTT Server and Configuration Management Server behaviour

The MCPTT Server and the Configuration Management Server apply required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [11].

The MCPTT Server and the Configuration Management Server achieve requested traffic reduction by implementation specific means. For example, the MCPTT Server or the Configuration Management Server may implement message throttling with prioritization or a message retaining mechanism for operations that can be postponed.

Diameter requests related to priority traffic (e.g., MCPTT emergency call), detected via the presence of priority information (e.g., Resource-Priority header field for MPS) in SIP messages as described in 3GPP TS 24.229 [13], have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests shall be the last to be throttled, when the MCPTT Server has to apply traffic reduction.

Annex B (Informative): Diameter overload node behaviour

B.1 Message prioritization

This clause describes possible behaviours of the MCPTT Server and the Configuration Management Server regarding message prioritization in an informative purpose.

The MCPTT Server may take the following into account when making throttling decisions:

- Identification of the procedures that can be deferred, so to avoid to drop non deferrable procedures;
- Prioritization of certain types of request (e.g. between NDR and DPR) according to the context of their use, in particular:
  - Lower prioritization of commands for MCPTT Server that are related to massive subscription data update due to provisioning.
  - Priority level of a priority user.

The Configuration Management Server may take the following into account when making throttling decisions:

- Identification of the procedures that can be deferred (e.g. Update of the MCPTT User Profile in the MCPTT database), so to avoid to drop non deferrable procedures;
- Prioritization of certain types of request (e.g. between NDR and DPR) according to the context of their use, in particular:
  - Lower prioritization of commands for the Configuration Management Server that are related to massive subscription data update due to provisioning.
  - Priority level of a priority user.

Annex C (normative): Diameter message priority mechanism

C.1 General

IETF draft-ietf-drmp-03 [8] specifies a Diameter message priority mechanism that allows Diameter nodes to indicate the relative priority of Diameter messages. With this information, other Diameter nodes may leverage the relative priority of Diameter messages into routing, resource allocation, and also abatement decisions when overload control is applied.

C.2 MCPTT-2 and CSC-13 interfaces

C.2.1 General

The Diameter message priority mechanism is an optional feature.

It is recommended to make use of IETF draft-ietf-drmp-03 [8] over the MCPTT-2 and CSC-13 interfaces of an operator network when the overload control defined in Annex A is applied on these interfaces.

C.2.2 MCPTT Server and Configuration Management Server behaviour

When the MCPTT Server and the Configuration Management Server support the Diameter message priority mechanism, the MCPTT Server and the Configuration Management Server shall comply with IETF draft-ietf-drmp-03 [8]. In particular, when priority is required, the MCPTT Server and the Configuration Management Server shall include the DRMP AVP indicating a priority level in the requests it sends and prioritise received requests according to priority level received within the DRMP AVP. It shall prioritise received answers according to the priority level received within the DRMP AVP if present, otherwise according to the priority level of the corresponding request. It shall include the DRMP AVP in the answer to a received request if the priority of the answer is different from the one of the request.

Diameter requests related to priority traffic (e.g. MCPTT emergency call) shall contain a DRMP AVP with a high priority of which the level value is operator dependent.

When not-explicitly requested, the inclusion and priority value of the DRMP AVP in Diameter messages are implementation specific.

C.2.3 MCPTT User Database behaviour

When the MCPTT User Database supports the Diameter message priority mechanism, the MCPTT User Database shall comply with IETF draft-ietf-drmp-03 [8]. In particular, when priority is required, the MCPTT User Database shall include the DRMP AVP indicating a priority level in the requests it sends and prioritise received requests according to priority level received within the DRMP AVP. It shall prioritise received answers according to the priority level received within the DRMP AVP if present, otherwise according to the priority level of the corresponding request. It shall include the DRMP AVP in the answer to a received request if the required priority of the answer is different from the one of the request.

When not explicitly requested, the inclusion and priority value of the DRMP AVP in Diameter messages are implementation specific.

Annex D (informative): Change history

Date	TSG #	TSG Doc.	CR#	Rev	Subject/Comment	In	Out
Feb 2016	CT4#72	C4-161515			Creation	0.0.0	0.1.0
Feb 2016	CT4#72	C4-161516			Version after Ct4#72	0.1.0	0.2.0
Mar 2016	CT#71	CP-160120			Presented for information and approval	0.2.0	1.0.0
Mar 2016	CT#71	CP-160162			TS number added and Approved	1.0.0	1.0.1
Mar 2016	CT#71				Version 13.0.0 created after CT plenary	1.0.1	13.0.0
Jun 2016	CT#72	CP-160227	0001	2	Enhancements to MCPTT-2 and CSC-13	13.0.0	13.1.0
Jun 2016	CT#72	CP-160227	0002	2	IANA assigned application Id and command code values	13.0.0	13.1.0

History

Document history		
V13.0.0	May 2016	Publication
V13.1.0	August 2016	Publication